STATEMENT

OF

Doug Wagoner

on behalf of the

Security Clearance Reform Coalition

BEFORE THE

HOUSE COMMITTEE ON GOVERNMENT REFORM

July 13, 2006

Mr. Chairman and Members of the Committee, my name is Doug Wagoner and I am the President of DSA, Inc., a Northern Virginia-based information technology small business that requires clearances for our personnel supporting the National Security mission. I am speaking today as the Chairman of the Intelligence Committee of the Information Technology Association of America and as a spokesman for the Security Clearance Reform Coalition.

We would like to thank you for giving us this opportunity to appear before you once again to discuss the industry perspective on the continued shortcomings of the federal personnel security clearance granting process.

Our coalition, comprised of the Aerospace Industries Association, AFCEA International, the Associated General Contractors of America, the Association of Old Crows, the Contract Services Association, the Information Technology Association of America, the Intelligence and National Security Alliance, the National Defense Industrial Association

and the Professional Services Council, represents thousands of companies that provide products, services and support personnel to the federal civilian, defense and intelligence communities. Our focus here today is on those personnel supporting vital National Security programs and efforts that require a clearance.

The Coalition compliments the President for extending the authority of Executive Order 13381 for an additional year and applauds and supports the adoption and implementation of the updated December 2005 President's Adjudicative Guidelines for Determining Eligibility for Access to Classified Information as a vital reform necessary for the eventual attainment of consistent clearance outcomes that support clearance reciprocity across the government. For too long, clearances have not been reciprocally recognized from agency-to-agency, department-to-department and even between agencies within the same department. At the root of the problem is an inherent lack of trust between agency adjudicators, each one thinking that they alone can evaluate and determine a person's trustworthiness for a clearance

granting access to the classified information they control. These revised Guidelines are the latest iteration of a longstanding effort to get agencies and departments to adopt uniform criteria for determining whether or not to grant a clearance.

Unfortunately, although the President issued the revised guidelines in December 2005, they have yet to be uniformly adopted or applied across government. We continue to experience problems regarding the equitable application of adjudicative criteria and the reciprocal acceptance of those criteria across agencies, and this lies at the heart of the problem. If agencies can be confident that all of the federal agencies adjudicate to the same criteria and standard, they should have confidence recognizing a clearance issued by another agency for the same level of access. That is sadly not the case. It is worth noting, however, that efforts are underway to bring about change and industry would like to recognize and thank Mr. Bill Leonard, the Director of the Information Security Oversight Office, for his continued leadership in the issue of reciprocity in the clearance granting process.

The application of criteria regarding the foreign influence on an applicant is especially important to our Coalition member companies because of the many gifted technical personnel with foreign connections who can provide valuable help to our National Security missions. Other clearance applicants are singled out because of family or marital ties to foreign nationals or because they may be considered to be a dual citizen based merely on their birth abroad to US parents. America cannot deny itself access to this talent. There is the anecdotal case of the U.S. military general, who, upon retirement, applied to have his clearance transferred to his new place of employment and was rejected because he was married to a Canadian national. The nationality of his spouse was never a disqualifier during his military service, yet the same person working for industry apparently was no longer considered trustworthy. Unfortunately, the more frequent response is to reject applicants with such conditions without any viable measurement of the actual risk they might pose during the adjudication process. Part of this problem can be attributed to the lack of training for adjudicators, some of which is classified,

regarding the degree of risk presented by certain foreign nations. This measurement of risk would include the intelligence/counterintelligence infrastructure of a nation and the ability or history of applying coercion or pressure by that nation to U.S. citizens with relatives or friends residing in the country. Before the end of the Cold War, there was a list of "designated countries," i.e. those whose interests were clearly inimical to the U.S., which adjudicators could use to assist them in rendering a decision. Since many countries who used to be on that now discontinued list are today allies of the U.S., these decisions must be made on a case-by-case basis depending on the country.

Evaluating the extent of a person's foreign connections as part of the investigative portion of the clearance granting process is one of the weakest links in the entire effort. Applications that raise issues regarding foreign interaction routinely wait months before being investigated, thereby creating a significant delay in the process. Because these "parked" applications are essentially invisible in the process, they also create much uncertainty for the applicant and the

employer. As part of its' investigative process, the Office of Personnel Management (OPM) continues to queue up applications for foreign investigations, only working on them when enough tied to a particular country have accumulated.

That is not good enough and other government agencies appear to agree. The Department of State specifically sought and received approval to establish their own investigative and clearance granting program after they evaluated the OPM process and found it lacking to meet it's needs. State electronically sends out queries regarding clearance applications it is handling as they are received. As a result, the Department of State personnel security program may already meet - if not exceed - the ambitious timelines mandated by the Intelligence Reform Act of 2004. Industry is unable to comprehend why OPM cannot either duplicate the State Department electronic transmission process or, even better, contract with the State Department to utilize their "best practice" system when foreign checks on an applicant are necessary.

Government oversight of adjudication is itself sometimes part of the problem. The Defense Industrial Security Clearance Office (DISCO), an office of the Defense Security Service, and other DoD Central Adjudication Facilities, have in the past routinely adjudicated cases which had been closed pending on some relatively minor investigative lead by either DSS or OPM, such as the FBI name check (vice criminal history check), with the rest of the case favorably completed. However, since the Government Accountability Office has previously criticized DoD for granting clearances on cases that do not fully comply with the national guidelines, DoD has directed that OPM not return any case for adjudication unless all leads have been completed. This development has caused many cases to be held at OPM that otherwise could have been favorably adjudicated on a risk management basis pending completion of some relatively minor lead in a case. While this approach assures complete adherence to the letter of the investigative guidelines, it precludes individuals from being issued a clearance based on an otherwise favorable investigation where the risk is minimal to non-existent.

In conclusion, our Coalition makes two recommendations that we believe will foster further reform of the federal personnel security clearance process. Both of these steps revolve around the clear direction Congress provided for improving the process in the 2004 Intelligence Reform and Terrorism Prevention Act. This direction established viable milestones for the improvement of the clearance granting process. However, agency failure to adopt and implement those standards is one of the reasons this Committee has convened twice in the last few months.

First, we recommend the creation of an agency-sponsored "pilot program" that would utilize technology and government and industry best practices for the application and investigation stages of the clearance granting process, including periodic reinvestigation. Since standards and criteria currently exist and are widely used across government and industry for these two functions, there is no inherent governmental role at these stages of the process. Industry believes that the efficiencies of such a pilot program would provide a clear

contrast to the antiquated technology and the Eisenhower-era, paperwork intensive processes currently in use by OPM and others. To create a means of comparison with existing processes and to measure the effectiveness of such a pilot program, the same applications entered into the pilot program would also be submitted to the existing clearance granting process. For example, a statistically valid sample of investigations or reinvestigations could be selected for a parallel test of 1) the standard OPM investigation, and 2) an investigation utilizing, among other things, automated applications, electronic submission of fingerprints and signatures and verification of investigative criteria using commercial and government databases and telephonic contacts. Testimony today does not provide sufficient time to detail such a proposal, but industry stands ready to work closely with the Committee and its staff to develop such a proposal, including how it can reduce the backlog of clearances, lower the costs to government, and use new case management technologies to expedite and improve the efficiency of the clearance process.

Second, we recommend evaluating the application, investigation, adjudication and reciprocal recognition stages of the clearance granting process for each agency against the legislatively mandated criteria of the 2004 Intelligence Reform Act and take appropriate action identified in the law, including the suspension or revocation of the ability to grant clearances. Obviously, such an action would be in the extreme, but we are not aware that such metrics are being measured or evaluated and therefore, there is no viable mechanism to identify where the weaknesses persist. A "stoplight" grading process – much like that currently employed to evaluate success under the President's Management Agenda - for all investigative and adjudicative agencies would be a sufficient first step to recognize success and best-practices where they have been developed and adopted and to single out those areas that are in need of greater support and attention.

Obviously, these recommendations would require a continued strong commitment from Congress and the Administration to see the clearance process reformed. An end-to-end evaluation for each

agency that submits applications and adjudicates clearances would provide transparency to the process and allow us to really focus resources. A pilot program would provide an opportunity for government and industry to work together to demonstrate that technology and automation can work to cut the red tape of the personnel security clearance process. Achieving the goal of reform is vital to ensuring that the contractor workforce is ready and able to support the National Security mission.

On behalf of the ITAA Intelligence Committee and the Security Clearance Reform Coalition, I wanted to thank you again for the opportunity to testify before you today. I am happy to answer your questions.